

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

HTC Cellular Phone, S/N: HT7150400107, MEID:
99000725127740, Number: 262-484-8036 in the U.S.
Probation evidence room safe.

Case No. 18-M-198 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 2252

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

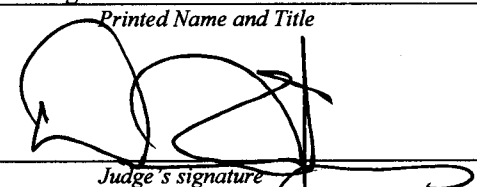

Applicant's signature

FBI Special Agent Eliot Mustell

Printed Name and Title

Sworn to before me and signed in my presence:

Date: Nov. 28, 2018


Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Eliot Mustell, being duly sworn on oath, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a HTC phone as described in Attachment A, which is currently in law enforcement possession, and the extraction from that property of the electronically stored information described in Attachment B.
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI). I have been employed with the FBI since June 2013. I am assigned to the FBI's Child Exploitation Task Force, Milwaukee Division. My duties include investigating violations of federal criminal law, including violations of Title 18, United States Code, Section 2251, which criminalizes producing child pornography, and Section 2252, which criminalizes accessing with intent to view, possessing, receiving, and distributing child pornography. I have gained experience in conducting these investigations through training and through everyday work, including executing search warrants and conducting interviews of individuals trading and manufacturing child pornography. I have also received Internet Crimes Against Children (ICAC) training, which includes training in investigating and enforcing state and federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography.
3. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers and FBI employees, who have provided information to me during the course of their

official duties and whom I consider to be truthful and reliable. This affidavit is also based upon information gained from interviews with cooperating citizen witnesses.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

5. On August 11, 2018, SA Mustell received a report from U.S. Probation that detailed a 2007 child pornography investigation involving an individual who is still under federal supervision. U.S. Probation provided the report from 2007, which contained the following information:
6. On or about August 21, 2007, an Australian Federal Police undercover operative (UCO) detected a posting in a chat room by the user of the email address talon_fei@yahoo.com. The posting invited anyone who has pornography involving babies to contact him, at the screen name "gekiblu" on "Hello" Google. The UCO contacted "gekiblu," and during the chat conversations "gekiblu" stated that he was looking for hardcore videos involving babies. "[G]ekiblu" said he was interested in children 0-12 years of age but stated, "I love babies."
7. The UCO adopted the persona of a 32 year old mother with two children. During the chat session, "gekiblu" repeatedly asked about the UCO's children and asked if she had committed contact offenses with her children. Without being requested, "gekiblu" transmitted to the UCO, during the chat sessions, a total of 63 still images and four videos. These images consist of babies who have penises in their mouths, semen on them, are having their genitalia exposed, and are being vaginally and anally penetrated. Other images

depict babies that are urinating and defecating on themselves. One of the video files is titled "3 Gets leverway" and is a 5:50 minute video of prepubescent girls engaged in oral, vaginal, and anal sex with an adult male.

8. "[G]ekibblue" commented on several of the images that he sent. Images where toddler females had their genitalia exposed were accompanied by comments such as, "I love this pussy," "look at this sweet pussy," and "yummy." During the chat with the UCO, "gekibblue" claimed to be 21 years old and working at Disney, near Orlando, Florida. "[G]ekibblue" also indicated that his screen name was taken from the Japanese television show "Gekiranger."
9. The UCO conducted an internet search on the e-mail address talon_fei@yahoo.com. The results showed a MySpace account belonging to a 21 year old male named "Tony." "Tony" worked at Disney-MGM and lived in Kissimmee, Florida. "Tony" graduated from high school in Deltona, and was part of the Japan Club.
10. Based on this information, on August 22, 2007, subpoenas were issued to both Yahoo! and Google. Yahoo! and Google subsequently provided an IP address that enabled the agents to locate the defendant's physical address of 4492 Saint George's Court, Kissimmee, Florida. On August 27, 2007, agents obtained a search warrant for this address. On August 28, 2007, agents conducted a search at 4492 Saint George's court, Kissimee, Florida. Tony Guerra was at the residence at the time of the search. Guerra agreed to a non-custodial interview with the agents.
11. Guerra stated that he was the roommate of Adam "AJ" Roebke. Guerra stated that he resided at Roebke's residence since June 2007. Guerra advised that his email address was

talon_fei@yahoo.com and his screen name was "gekiblue." Guerra advised that he had been chatting on "Hello" Google daily. Guerra stated that during those chats, he received and distributed images of child pornography. Guerra further advised that the last time he had received and distributed images of child pornography was the night before the execution of the search.

12. On August 29, 2007, a preliminary forensic exam on the computer used by Guerra was conducted. The computer contained over 5,000 images of child pornography. According to the FBI Agent, the images were all prepubescent children, in his opinion, being no more than six years old. One of the images contained a newborn baby with an umbilical clamp still attached. In addition, many "chats" were recovered from the computer. Following are excerpts from some of the chats Guerra had with other individuals over the internet.

13. The following chat took place on August 21, 2007, at approximately 4:44p.m., with "outlawjessejames."

- outlawjessejames: what u into with kids
- gekiblue: I havent done anything
- gekiblue: I'm a pedo virgin lol
- outlawjessejames: /u should try
- gekiblue: I wish I could
- outlawjessejames: why cant you
- gekiblue: No kids around
- gekiblue: Oh you gonna have a cam? By then
- outlawjessejames: hoping

- gekibblue: oh ok cool
- outlawjessejames: what you would want me to do on cam to her
- gekibblue: anal pussy oral fisting *lol*
- outlawjessejames: force sex too right
- gekibblue: oh heavy rape
- outlawjessejames: thas me
- gekibblue: nice do you have a microphone?
- outlawjessejames: nope but her face be on cam
- gekibblue: I want to hear her sceAM LOL
- outlawjessejames: if they old enuff to wear panties old enuff to be fucked
- outlawjessejames: and her
- gekibblue: old enough to be in diapers is wat I say

14. Tony Guerra was arrested by federal authorities on August 30, 2007. On August 31, 2007, Guerra appeared before the U.S. Magistrate Judge Gary R. Jones for his initial appearance and was temporarily detained. Tony Guerra was arrested by federal authorities on August 30, 2007. On August 31, 2007, Guerra appeared before the U.S. Magistrate Judge Gary R. Jones for his initial appearance and was temporarily detained.
15. On November 5, 2008, Mr. Guerra appeared before the Honorable Mary S. Scriven in the Middle District of Florida. He was sentenced to 130 months in the Bureau of Prisons for Receipt and Distribution of Child Pornography. Mr. Guerra commenced a Life term of

supervised release on 2/4/17. On March 16, 2018, Judge J.P. Stadtmueller approved a transfer of jurisdiction, transferring Mr. Guerra's case to the Eastern District of Wisconsin.

16. On May 4, 2018, an unscheduled contact was made with Mr. Guerra at his residence, 8743 Sheridan Road, Kenosha, Wisconsin, by U.S. Probation Officer Jennifer Cravatta. At that time, contact was made with Mr. Guerra and he admitted to accessing the following websites and applications on his cell phone: imagesource.ru, sharechann, nonuchan.net, Dropbox, Omegle, Kik, and Snapchat. Also at this time, he admitted to communicating with females, ages 12 to 17 years old, on Kik and Snapchat and received their nude photos. On May 7, 2018, Mr. Guerra reported to the U.S. Probation Office, 517 E. Wisconsin Avenue, Milwaukee, Wisconsin with his cell phone. While at the office, he was interviewed by Officer Cravatta and U.S. Probation Officer Andrew Cieslewicz. At that time, Mr. Guerra admitted to accessing videos of females, ages 10 to 12 years that were posing nude. He stated he would chat with individuals on Omegle and would get links to videos to watch and/or download. He stated he would get links via Dropbox for the videos. Officer Cieslewicz asked Mr. Guerra to access the videos on his phone, but he indicated he had deleted them prior to reporting to the probation office. Officer Cieslewicz did observe the following Google search history on the phone by scrolling through his internet history: talking Arabic translator, Preggo Instagram, Sharechanncom, Haley lynn, Free pregoo galleries, Mrvinen, Rock county job center, and Foods stamps in Janesville. Additionally noted was archived search history of the following: animal sex cams, beast cams, frostwire torrent, Gfet: kinky fetish BDSM Dating & Gay Fet Lifestyles, aahchat.org, Kid chat rooms under 13, Topless, photo of mom & 14 year old daughter, I'm a 12 year old girl and single,

parentingpassage.com, and girls potty train. The phone and charger was seized from Mr. Guerra, placed on airplane mode, and secured in the U.S. Probation Office's evidence safe by U.S. Probation Officer Megan Cleveland.

17. On August 10, 2018, SA Mustell received an email from U.S. Probation Officer Andrew Cieslewicz. In the email, Officer Ciezlewicz stated his office seized the smart phone from Mr. Guerra, who verbally admitted to accessing/viewing child pornography on it. Mr. Guerra was asked to show the U.S. Probation officers the child pornography, but Mr. Guerra stated he deleted the material. U.S. Probation officers noted the following on the phone when meeting with Mr. Guerra within the Google search history:

- talking Arabic translator
- Preggo Instagram
- Sharechanncom
- Haley lynn
- Free pregoo galleries
- Mrvinen
- Rock county job center
- Foods stamps in Janesville
- animal sex cams
- beast cams
- frostwire torrent
- Gfet: kinky fetish, BDSM Dating & Gay Fet Lifestyles
- aahchat.org
- Kid chat rooms under 13
- Topless photo of mom & 14 year old daughter
- I'm a 12 year old girl and single
- parentingpassage.com [with photo of child bathroom training]

- girls potty train

DEFINITIONS

18. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

- a. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- b. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
- c. "Computer Server" or "Server" is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.
- d. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- e. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- h. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).
- i. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- j. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

19. *Electronic storage.* Based on my training and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device used to access them. This

information can often be recovered with forensic tools. There is probable cause to believe that things that were once stored on the device in Attachment A may still be stored there, for at least the following reasons:

- a. Based on my training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can often be recovered using forensic tools. This is so because when a person “deletes” a file on an electronic storage device, the data contained in the file does not actually disappear. Rather, that data remains on the storage medium until it is overwritten by new data.
- b. Deleted files, or remnants of deleted files, may reside in free space or slack space –space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, an electronic device’s operating system may keep a record of deleted data in a “swap” or “recovery” file.
- c. Files that have been viewed via the Internet are often automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages, or if a user takes steps to delete them.
- d. Computer storage media, in particular internal hard drives, contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. Though technically possible, computer users typically do not erase or delete this evidence because special software is typically required for that task.

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crime described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a

paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. Based on my training and experience, I know that when an individual uses a computer to commit crimes involving child exploitation and pornography, the individual’s computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain: data that is evidence of how the electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

21. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit examinations of the Device consistent with the objects of the warrant. These examinations may require computer-assisted scans of the entirety of the device, which may be followed with human inspection of the results in order to determine whether they contain the types of evidence described by the warrant.

22. *Manner of execution.* Because this Application seeks only permission to examine the Device already in law enforcement's possession, the execution of this warrant does not involve an intrusion onto any physical premises. Therefore, it is reasonable for the Court to authorize the execution of the warrant at any time in the day or night.

CONCLUSION

23. For these reasons, I submit that the information set forth in this Affidavit provides probable cause to believe that the Device described in Attachment A to this Application contains evidence, as described in Attachment B of this Application, of the crimes of possession and receipt of child pornography, in violation of Title 18, United States Code, Section 2252, et seq.

ATTACHMENT A

Property to Be Searched

Brand: HTC
S/N: HT7150400107
Software version: 1.32.651.11
Hardware version: 0004
MEID: 99000725127740
Number: 262-484-8036
No pin needed to unlock phone

The phone is in the U.S. Probation evidence room safe with airplane mode on.

ATTACHMENT B
Items to Be Seized

Your Affiant seeks to forensically search the Device in Attachment A and to seize and preserve as evidence any of the below-listed items:

1. All records that relate to violations of Title 18, United States Code, Section 2252, et seq.; Title 18, United States Code, Sections 2423, et seq.; Title 18, United States Code, Section 2422(b); and Title 18, United States Code, Section 1470, including but not limited to:
 - a. GPS and other location data in any form, including records of the use of navigational applications and file metadata;
 - b. Records of calendars, scheduling notes or applications, or other evidence of travel plans;
 - c. Records of the Device's Internet activity, including firewall logs, caches, browser history, cookies, bookmarked or favorited web pages, user-entered search terms, and user-typed web addresses;
 - d. Records of any online multiplayer games accessed or installed on the Device;
 - e. Records of the use of the FaceTime application on any Apple devices;
 - f. Any photographs or videos of any minors, including any such images that would constitute child pornography or erotica;
 - g. Electronic communications regarding the crimes under investigation, including text messages, emails, chats and messages within online games and social media applications; and
 - h. All call logs that may relate to the crimes under investigation.
2. Evidence of how, when and where the Device was used, including but not limited to:
 - a. Records of Internet Protocol (IP) addresses used by the Device;
 - b. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. Evidence of the absence of such malicious software;

- d. Evidence indicating how and when the Device was accessed or used to determine the chronological context of access, use, and events relating to the crimes under investigation;
 - e. Evidence that any removable storage devices or similar container for electronic evidence was at one time attached to the device, such as a USB drive or an external hard drive;
 - f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Devices; and
 - g. Any encryption keys.
3. Evidence of user attribution, showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted. This may include such records as call logs, phonebooks, saved usernames and passwords, documents, electronic communications, and browsing history.

As used above, the term "records" includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.